Suchmaschinen im Internet bereits automatisieren. Warum also nicht nach Mailadressen suchen?

Surfen Sie gerne im Internet? Haben Sie schon „heiße“ Server besucht (ja, aber nur kurz)? Haben Sie für eine „freie Mailbox“ bei x.y einen Fragebogen ausgefüllt? Sie ahnen es, damit ist Ihre Mailadresse bekannt, eventuell auch etwas zu Ihren beruflichen Absichten, Betätigungsfeldern usw. Von dort ist es eigentlich nur noch ein kleiner Schritt, daß diese Informationen vermarktet werden können.

Nutzen und Mißbrauch der elektronischen Kommunikation liegen dicht beieinander, den perfekten Schutz wird es nicht geben. Das kommt mir irgendwie bekannt vor, haben Sie etwas anderes erwartet?

Burckhard Schmidt

Umgang mit Paßwörtern
Die Sorgen der Benutzerberatung

In diesem Artikel sollen einige Aspekte der Arbeit der Benutzerberatung des Rechenzentrums hinsichtlich der Thematik dieses Heftes beschrieben werden. Gerade wir als Benutzerberatung sind in den meisten Fällen der erste Ansprechpartner der Benutzer, haben die oft undankbare Aufgabe, Sicherheitsanforderungen durchzusetzen und sind nicht selten dem verständnislosen Zorn eines Mitarbeiters oder Studierenden der HU ausgesetzt, dessen Account wegen einer nicht durchgeführten Paßwortänderung oder eines anderen „Vergehens“ gesperrt wurde. Wir müssen jedoch immer wieder feststellen, wie erschreckend groß die Defizite im Sicherheitsbewußtsein vieler Benutzer sind, wie unbekümmert Paßwörter an andere weitergegeben werden (Teilweise werden sie sogar per E-Mail verschickt!) und wie wenig Klarheit darüber herrscht, welche Folgen ein derart leichtfertiger Umgang mit dem eigenen Account haben kann.

Als wir zum Sommersemester 1995 begannen, für Studierende einen im Vergleich zu den vorangegangenen Jahren erheblich vereinfachten persönlichen Zugang zum Internet über einen UNIX-Account anzubieten[1], waren Probleme hinsichtlich der Sicherheit des Netzes in diesem Umfang noch kein Thema für uns. Als einzige Sicherheitsmaßnahme wurde die Änderung des Paßwortes beim ersten Login erzwungen, was durch das Kommando *passwd* in der Datei *.login* realisiert war. Die zunächst überschaubar geringe Zahl der eingetragenen Benutzer stieg erwartungsgemäß rasant an (gegenwärtig liegt sie bei ca. 12.000), und auch die ersten massiven Hacker-Attacken ließen nicht lange auf sich warten.

Die Angriffe konzentrierten sich u. a. auf das Entschlüsseln von Paßwörtern. Diese werden im Betriebssystem UNIX chiffriert gespeichert. Durch eine Schwäche des bei uns eingesetzten Account-Verwaltungssystems NIS (Network Information System) ist es jedoch relativ einfach möglich, die chiffrierte Form eines Paßwortes zu lesen. Hacker benutzen sog. Crack-Programme, die mit umfangreichen Wörterbüchern arbeiten, jedes darin enthaltene Wort verschlüsseln und mit den im NIS gespeicherten Einträgen vergleichen. So können Paßwörter herausgefunden werden, die z. B. nur aus einem Wort der englischen oder deutschen Sprache bestehen. Um dem zu begegnen, begannen wir, selbst solch ein Crack-Programm laufen zu lassen. Zunächst wurden die Benutzer, deren Paßwort von diesem Programm ermittelt werden konnte, per E-Mail gebeten, ihr Paßwort zu ändern. Das hat sich bald als unzureichend erwiesen. Sehr viele Benutzer lesen ihre Mails nur in größeren Abständen, so daß wir uns gezwungen sahen, derart unsichere Accounts mit sofortiger Wirkung zu sperren. Die Benutzer wurden auf diese Art veranlaßt, sich mit uns in Verbindung zu setzen. „Sperren“ hieß dabei, dem Benutzer (und dem Hacker!) jeglichen Zugang zu dem Account zu verwehren. Gespeicherte Daten wurden davon nicht berührt, auch Mails konnten weiterhin empfangen werden. Die Sperre konnte durch das Rechenzentrum jederzeit wieder aufgehoben werden, wobei ein neues, sicheres Paßwort gesetzt wurde.

Im Herbst 1996 ersetzten wir das UNIX-Standard-Kommando *passwd* durch das Programm *anlpasswd*, das bereits beim Ändern des Paßwortes durch den Benutzer das neue Paßwort auf seine Sicherheit testet. Seitdem können zu einfach strukturierte Paßwörter gar nicht mehr in das System gelangen. Da es darüber hinaus viele Möglichkeiten gibt, ein Paßwort – mit oder ohne Absicht – in fremde Hände geraten zu lassen, kann auch ein relativ sicheres Paßwort nach einer gewissen Zeit nicht mehr als sicher gelten. Daher führten wir gleichzeitig die Regelung ein, daß jedes Paßwort halbjährlich zu ändern ist. Zusätzlich verlangten wir nach dem Einrichten neuer Accounts die Änderung des

1 Wendland, B.: Mit „amor“ ins Internet
RZ-Mitteilungen, Nr. 11, 1995, S. 23f.
http://www.hu-berlin.de/rz/rzmit/rzm11/rzm11_9.html

Anfangspaßwortes innerhalb von sechs Wochen. Hier zeigte sich eine weitere Unzulänglichkeit des NIS, nämlich die Tatsache, daß es kein Verfallsdatum für Paßwörter kennt. Es war also eine Eigenlösung gefragt, die darin besteht, daß die die Paßwörter enthaltene NIS-Datei täglich mit einer Kopie des Vortages verglichen wird. Das übernimmt ein automatisch ablaufendes Shell-Script. Für jeden Account wird ein Zähler geführt, der bei durchgeführter Paßwortänderung auf Null zurückgesetzt wird. Erreicht der Zähler den festgelegten Wert (6 Monate bzw. bei neu eingerichteten Accounts 6 Wochen), wird ebenso automatisch die Sperrung des betreffenden Accounts veranlaßt.

Ein weiterer Grund für das Sperren eines Accounts ist eine Weitergabe des Paßwortes an andere, was durch die Benutzerordnung des RZ sowie die Computerbetriebsordnung der HU ausdrücklich untersagt ist. Mit seiner Unterschrift hat sich jeder Benutzer bei der Account-Vergabe verpflichtet, diese Ordnungen einzuhalten. Hier steht natürlich die Frage im Raum, wie wir die Paßwortweitergabe feststellen. Schließlich ist die Auswertung der persönlichen Daten der Benutzer (E-Mail, Dateien im Homeverzeichnis usw.) durch die Bestimmungen des Datenschutzes strikt untersagt bzw. nur mit behördlicher Genehmigung gestattet. Abgesehen davon wäre eine diesbezügliche Überwachung schon rein technisch gar nicht möglich. Es lassen sich aber Rückschlüsse aus der Beobachtung der vom Benutzer hergestellten Netzverbindungen sowie der aktivierten Kommandos ziehen. Wenn ein Benutzer z. B. – bedingt durch einen Auslandsaufenthalt – regelmäßig eine Telnet-Verbindung aus den USA ins RZ herstellt, gleichzeitig jedoch Einwahlverbindungen über Modem erfolgen, ist die Begründung, er habe sich eben auch mal aus Kalifornien bei uns einwählen wollen, nicht sehr glaubhaft. Es ist jedoch naheliegend, daß dies nur Zufallstreffer sein können, so daß wir von einer erheblichen Dunkelziffer der Mißbräuche ausgehen müssen.

Der Inhaber eines wegen Paßwortweitergabe oder eines anderen Verstoßes gegen die Benutzungsbedingungen gesperrten Accounts gibt eine schriftliche Stellungnahme ab. Der Account wird im Normalfall nach einem Hinweis auf die Benutzungsbestimmungen mit einem neu gesetzten Paßwort wieder freigegeben. Im Wiederholungsfall droht dem Benutzer die dauerhafte Sperrung seines Accounts. Wurde der Account wegen eines nicht geänderten Paßwortes gesperrt, muß der betreffende Benutzer persönlich mit uns in Kontakt treten und sich ein neues Paßwort geben lassen.

Wie diese Ausführungen zeigen, ist die Benutzerberatung des Rechenzentrums mit den o. g. Maßnahmen bestrebt, die Sicherheit des Systems ständig zu erhöhen sowie die Sensibilität der Benutzer diesbezüglich zu entwickeln.

Bert Wendland
bert=wendland@rz.hu-berlin.de